



DEPARTMENT OF THE ARMY

HEADQUARTERS, FORT HOOD
1001 761ST TANK BATTALION AVENUE
FORT HOOD, TEXAS 76544-5000

REPLY TO
ATTENTION OF

AFZF-GT

JUL 12 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: III Corps and Fort Hood Operations Security (OPSEC) and Network Defense Measures

1. Recent network intrusions and system compromises at Fort Hood raise serious concerns regarding our ability to withstand cyber attacks. We are an Army at war--protecting sensitive information on our networks is one of the most critical force protection tasks we have. Failure to protect that information gives the enemy a vote in interdicting our operations and endangers the lives of our Soldiers and our loved ones. We must deny our enemies--foreign and domestic--the opportunity to have that vote.
2. With limited resources at the Army level to assure security of the Fort Hood network, we are the first and often last line of defense. Therefore, it is essential that commanders, senior executives, and managers ensure compliance with the following tenets of our current information security policy:
 - a. All users must log into the Hood domain. No work groups or domains are authorized unless approved by the Director, Information Management (DOIM).
 - b. All automation devices will comply with the Department of the Army published Information Assurance Vulnerability Management (IAVM) directives and network security procedures.
 - c. Failure to follow proper cyber security policies will result in immediate suspension of network access and privileges.
 - d. Under no circumstances will a subscriber move, alter, place an attachment on, or make any additions to official telephone or internal local area network equipment including hubs, routers, switches, and any multi-port devices.

This is a leadership issue and I expect leaders at all levels to heed these instructions and to take the necessary measures to fix the Fort Hood computer network defense

AFZF-GT

SUBJECT: III Corps and Fort Hood Operations Security (OPSEC) and Network Defense Measures

and Operation Security posture. Your Information Assurance Security Officers (IASOs), Information Management Officers (IMOs), and Systems Administrators (SAs) are our first-line of defense and must have your unconditional support.

3. We will implement this program using the following tactics, techniques, and procedures:

a. Unannounced spot checks and inspections of network security procedures will be made both over the network and via on-site checks by command inspection teams.

b. All IASOs, IMOs, and SAs are to be tracked, trained, and reported as part of the unit's battle roster, just as you track tank crews and MCS operators.

c. Systems found on our networks that have failed to implement information assurance updates and other directed updates, modifications, or changes will be removed from the network **immediately**.

d. Failure to implement the above programs will be dealt with sternly. Inspection results, failures to maintain information assurance battle rosters, and removal from the network will be reported as command interest items to me, the Commanding General, Fort Hood. Systems removed from the network will only be restored upon the approval of my designated OPSEC representative or me.

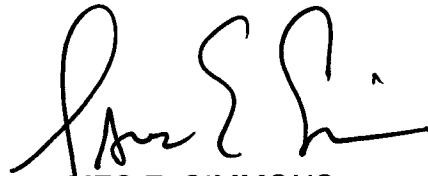
e. All Fort Hood personnel who have computer user accounts must obtain a license to be granted access to the Fort Hood Installation local area network. Licenses are earned with a score of 80 percent or better on the Fort Hood computer users test. The DOIM is charged with developing, implementing, and administering the computer users test.

Having a computer network and automation system is a privilege, not a right. They are critical tools in fighting this Global War on Terrorism. Your task, as leaders, is to ensure that we train, maintain, and sustain these capabilities, as well as protect them. I charge you--not your S6s, DOIM, or any other agency--with that responsibility and with ensuring that government computers are used for their intended, official purposes.

AFZF-SGS

SUBJECT: III Corps and Fort Hood Operations Security and Network Defense Measures

4. This is first, and foremost, an OPSEC issue. Therefore, I charge the G3, as the staff lead for OPSEC, to establish immediately an OPSEC and network protection team comprised of the DOIM, Corps G3 OPSEC, G2, G6, and Force Protection to review our policies, implement the command inspection program, and to stand-up our tracking and reporting system. The points of contact for this effort are the III Corps (R) G3, Mr. John Diem, (254) 287-2203, and G3 OPSEC noncommissioned officer in charge, Staff Sergeant J. Varner, (254) 288-3113.

A handwritten signature in black ink, appearing to read 'James E. Simmons', with a stylized flourish at the end.

JAMES E. SIMMONS
Major General, USA
Commanding

DISTRIBUTION:

IAW FH Form 1853: A